

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

WELLS FARGO & COMPANY, a Delaware
corporation, WFC HOLDINGS
CORPORATION, a Delaware corporation,
and QUICKEN LOANS, INC., a Michigan
corporation,

Plaintiffs,

vs.

WHENU.COM, INC., a Delaware corporation,

Defendant.

Case No. 03-71906

Hon. Nancy G. Edmunds
Magistrate Judge Pepe

2003 OCT -9 P 4:15
U.S. DIST. COURT CLERK
EAST DIST. MICH.
DETROIT

FILED

DEFENDANT WHENU.COM'S MEMORANDUM OF LAW
IN SUPPORT OF CONTINUING THE ORDER SEALING
THE DECLARATION OF BENJAMIN EDELMAN AND TRANSCRIPTS
OF CERTAIN TESTIMONY OF AVI NAIDER AND MR. EDELMAN

PRELIMINARY STATEMENT

Plaintiffs filed a motion for a preliminary injunction on May 20, 2003, and defendant WhenU ("WhenU") responded to that motion on June 23, 2003. In their reply papers, plaintiffs submitted a declaration of Benjamin Edelman, dated July 11, 2003, that revealed confidential information about defendant's proprietary software (PX 109) (the "Edelman Declaration"). Immediately upon receiving the Edelman Declaration, WhenU brought an emergency motion for an order sealing it. On July 17, 2003, following a telephonic hearing, the Court sealed the Edelman Declaration pending the hearing on the preliminary injunction motion. Later that day, plaintiffs moved for reconsideration, and submitted a second declaration from Mr. Edelman, dated July 17, 2003 (PX 186). Defendant opposed the motion and submitted a

4-

declaration from WhenU's CEO Avi Naider in support of its opposition (DX 538). On August 12, 2003, the Court denied Plaintiffs' motion.

At defendant's request, the Court also placed portions of the transcript of Mr. Edelman's and Mr. Naider's testimony under seal, pending the completion of the hearing. At the conclusion of the hearing, the Court requested that the parties brief the issue of the continuation of the sealing order.

STATEMENT OF FACTS

The SaveNow program is comprised of a three-part architecture: (a) a binary executable file, that, among other tasks, controls the physical display of SaveNow advertisements; (b) an obfuscated JavaScript source code that houses the proprietary business logic controlling the operation of the software (the "Control Code"); and (c) a scrambled directory that contains basic data and data mappings used by SaveNow (the "Directory") (collectively, the "SaveNow Code"). DX 538, ¶4. The SaveNow Code is confidential, proprietary information of WhenU. DX 538, ¶ 6. The way in which the SaveNow Code works, including details discussed in the sealed declaration and testimony, is not known to the public. Tr. VII (Naider) 71:24-72:5. In particular, it is not known to WhenU's competitors, and its revelation would place WhenU at a business disadvantage. Tr. VII (Naider) 72:6-12.

WhenU takes reasonable measures to maintain the confidentiality of the SaveNow Code. The executable portion of the SaveNow Code is compiled, such that only a highly trained expert using specialized equipment – a decompiler – could disassemble it. Tr. IV (Edelman) 125:10-18. Mr. Edelman testified that even he lacked the ability to penetrate that portion of the SaveNow Code. Tr. IV (Edelman) 124:24-125:15.

Certain confidential source codes cannot be included in the executable files for reasons related to the stability and functionality of the program. These codes are written instead in JavaScript in the Control Code. Tr. VII (Naider) 72:13-73-8; DX 538 ¶ 5 (WhenU uses JavaScript coding for the Control Code of SaveNow because it provides a flexibility and functionality critical to the operation of WhenU's business). WhenU looked at various ways to encrypt this Control Code or otherwise protect it from reverse engineering and found that the most aggressive measure that could be used was "obfuscation." Tr. VII (Naider) 69:12-17; 73:9-24; DX 538, ¶ 7. The JavaScript obfuscator "renames JavaScript variables and functions to make it more difficult to determine the function and purpose of the code" (PX 109, ¶ 21 n.1) and makes the code "considerably hard[er] to understand." Tr. IV (Edelman) 132:8-9. *See also* Tr. VI (Edelman) 84:11-20; DX 538, ¶ 7 (significant technical skill required to decipher obfuscated code).

The Directory is scrambled on a user's computer, so that an ordinary user would find the contents unintelligible. Tr. VII (Naider) 69:20-22; DX 538, ¶ 10; *see also* Tr. VI (Edelman) 91:8-18. The SaveNow Code, including the Directory, reflects four years of work product, and WhenU keeps it strictly confidential. It is not shared with affiliates or advertisers. Tr. VIII (Naider) 33:4-22; Tr. VII (Naider) 69:9-22, 70:23-72:12.

To protect the confidentiality of the SaveNow Code, WhenU requires all users of the SaveNow software to accept the terms of a license agreement (the "License Agreement"). Tr. VII (Naider) 58:23-59:12; DX 538, ¶ 11. The License Agreement prohibits, among other things, "reverse engineer[ing]", or otherwise attempt[ing] to derive the source code for the software. *See* DX 510 (License Agreement).

ARGUMENT

In *Nixon v. Warner Communications*, 435 U.S. 589, 598 (1978), the Supreme Court held that “every court has supervisory powers over its own records and files.” Those supervisory powers grant the courts authority to restrict public access to court files under a variety of circumstances, including when the files in question could be used “as sources of business information that might harm a litigant’s competitive standing.” *Id.* Thus, the public interest in having full access to court documents must yield when “interests of privacy outweighs the public’s right to know.” *In re Knoxville News-Sentinel Co.*, 723 F.2d 470, 474 (6th Cir. 1983).

The same standards apply to access to testimony (and transcripts) as to other court records. *See, e.g., Brown & Williamson Tobacco Corp. v. Federal Trade Comm’n*, 710 F.2d 1165, 1178-79 (6th Cir. 1983) (public’s right of access to the courtroom is “not absolute”). As the United States Supreme Court explained in *Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 600 (1980), “Just as a legislature may impose reasonable time, place, and manner restrictions upon the exercise of First Amendment freedoms, so may a trial judge impose reasonable limitations upon the unrestricted occupation of a courtroom by representatives of the press and members of the public.”

A confidentiality interest need not rise to the level of a trade secret under state law in order to be subject to restricted access, so long as the information “might harm a litigant’s competitive standing.” *Nixon*, 435 U.S. at 598. *Brown & Williamson*, which held that courts could protect “privacy rights of participants” as well as actual “trade secrets,” did not hold to the contrary. The *Brown & Williamson* court simply held that mere harm to “reputation” was an

insufficient basis for a corporation to seek to protect non-trade secret information. *Id.* at 1179-80.

Thus, courts will consider the possibility that disclosure of information would unduly damage a party's business. *See, e.g., Tavoulareas v. Washington Post Co.*, 111 F.R.D. 653, 661 (D.D.C. 1986) (maintaining under seal deposition transcripts and exhibits in a libel case that contained confidential and sensitive business information about a party that would harm that party's competitive position); *Standard & Poor's Corp., Inc. v. Commodity Exchange, Inc.*, 541 F. Supp. 1273, 1275-78 (S.D.N.Y. 1982) (in action for a preliminary injunction, denying news service's application to open courtroom where "the overriding interest to be found in business confidences – protected by law as trade secrets – required a temporary reasonably restricted access to the Courtroom of members of the public"); *Zeneca Ltd. v. Pharmachemie B.V.*, 37 F. Supp. 2d 85, 86 n.1 (D. Mass. 1999) (noting that Magistrate Judge's Report and Recommendation was amended to remove certain confidential business information which was "not essential to an understanding of the reasoning behind the Court's recommendation" and disclosure of which "might harm [the plaintiff's] competitive standing."); *Willie Nelson Music Co. v. Comm'r of Internal Revenue*, 85 T.C. 914, 921-22 (T.C. 1985) (noting that confidential business information, such as pricing information, customer lists and trade secrets, requires protection).

In any case, the information at issue is a trade secret of WhenU. Under Michigan law, a trade secret is information "not being readily ascertainable by proper means" that is "the subject of efforts that are reasonable under the circumstances to maintain its secrecy." Mich Stat. Ann. § 445.1902. The efforts undertaken to maintain secrecy need only be reasonable under the relevant business circumstances, taking into account the need for "flexibility" and

“good business practice in today’s modern world.” *Merrill Lynch, Pierce, Fenner & Smith, Inc. v. Ran*, 67 F. Supp. 2d 764, 771-72 (E.D. Mich. 1999) (finding no waiver of trade secret protection where brokers were allowed to remove confidential information from Merrill Lynch offices and to dispose of it without shredding).

A. The Testimony of Mr. Edelman Which Reveals the Actual Workings of the SaveNow Code Should be Sealed

Plaintiffs have argued that Mr. Edelman’s declaration and testimony concerning the inner workings of the SaveNow Code should not be sealed because the information Mr. Edelman reviewed was publicly available, and his analysis of it was permitted under the License Agreement. Tr. IV (Edelman) 124:10-19.¹ The record reveals otherwise.

Mr. Edelman was able to decipher the Directory, which is scrambled when it is loaded onto a user’s computer, using a dedicated computer in his laboratory that was connected to an electronic recording device called a “packet sniffer.” Using the packet sniffer, Mr. Edelman could record data as it was being delivered over his Internet connection. Without the use of a device like a packet sniffer, a computer user has no way to “see” data being transmitted over the Internet. Tr. VI (Edelman) 85:19-87:17.

Were it not for the packet sniffer or some other special tool, Mr. Edelman conceded that the WhenU Directory would have been downloaded onto his computer scrambled, and the scrambled Directory would have been “unintelligible.” Tr. VI (Edelman) 91:16-18. Mr. Edelman also conceded that ordinary computer users do not use packet sniffers. Tr. VI (Edelman) 90:17-21.

¹ WhenU is prepared to review the transcript and the Edelman Declaration and designate the particular sections that are highly confidential. WhenU does not seek wholesale sealing of any part of the record.

Mr. Edelman also relied on a packet sniffer to obtain the Control Code. Using a packet sniffer, Mr. Edelman found an out-of-date unobfuscated version of the Control Code which had been inadvertently left by WhenU on one of its servers. Tr. IV (Edelman) 128:10-20; Tr. VI (Edelman) 163:23-164:3. The URL for this server is not a public URL and its existence is not published by WhenU. DX 538, ¶ 8. An ordinary Save Now user would not have known about the existence of this unobfuscated version of the Control Code, nor would he have had any information on how to locate it. DX 538, ¶ 9. The two-year old unobfuscated version of the Control Code had been left there by an oversight, and was immediately removed once WhenU learned about it from the Edelman Declaration. DX 538, ¶ 9.

Mr. Edelman used the out-of-date, unobfuscated version of the Control Code like the Rosetta Stone to understand the current, obfuscated Control Code. Tr. IV (Edelman) 131:11-24. As Mr. Edelman testified: "it's thanks to that version that I understand so much of what I do about the more current version, which has been processed through a Java script obfuscator." *Id.*²

Despite Mr. Edelman's expertise, the benefits of a dedicated computer, and a sophisticated laboratory with an elaborate set-up and special tools, Mr. Edelman did not figure out how the SaveNow software worked. He admitted on re-direct that the SaveNow Code is "a complicated piece of software," and that there were a number of things he was not able to piece together until *after* hearing Mr. Naider's extensive testimony about the inner workings of the SaveNow Code. Tr. IX (Edelman) 83:25-85:19, 87:12-88:1.

² Mr. Edelman testified on direct that it is possible to read obfuscated control code because the obfuscator merely takes away features such as indentations that make it harder to figure out where the line breaks are, and how the parts relate to each other. Tr. IV (Edelman) 131:25-132:13. On cross-examination, Mr. Edelman conceded that obfuscation also changes variables. Tr. VI (Edelman) 84:14-20.

Mr. Edelman acknowledged that he was familiar with the provisions of the License Agreement which prohibit reverse engineering the software. Tr. IV (Edelman) 126:13-22. But according to Mr. Edelman's testimony at the hearing, "reverse engineering" only "refers to a process of looking inside of a[n] .exe file, taking it apart, figuring out what it does." Tr. IV (Edelman) 126:12:17. Thus, according to Mr. Edelman's hearing testimony "reverse engineering" does not apply to "looking inside of" obfuscated Control Code or a scrambled Directory and "figuring out what it does."

But as Mr. Edelman acknowledged, Control Code is code; it just is not "ready to run" like executable code. Tr. IV (Edelman) 125:1-4. In fact, the Control Code is what actually determines what the user sees as a result of having the SaveNow software. Tr. VI (Edelman) 82:7-10. The Directory is an integral part of the SaveNow Code. Although Mr. Edelman thought it might be possible to understand the Control Code and the Directory separately, he acknowledged that he "used the two together to understand how the entire system works" (Tr. VI (Edelman) 82:13-24), and that two are "like peas in a pod." Tr. IV (Edelman) 136:12-24. *See also* Tr. VIII (Naider) 31:22-32:2.

Mr. Edelman's actions constitute reverse engineering of the SaveNow Code. As Mr. Edelman acknowledged, he subjected the SaveNow Code to extensive "hands-on testing" and a "detailed inspection" in order to learn how it works. PX 109, ¶ 19. Indeed, Mr. Edelman used a much broader definition of "reverse engineering" as a plaintiff in a recent lawsuit. In his complaint in that case, Mr. Edelman described "reverse engineering" as "a process used to gain access to the functional elements of a software program in order to learn how it works." Tr. VI (Edelman) 93:10-94:22. That is precisely what Mr. Edelman did here.

In sum, the measures taken by Mr. Edelman to obtain and decipher the SaveNow Code were not within the knowledge or expertise of most Internet users. But for the special lab, packet sniffer and the old unobfuscated version of the Control Code Mr. Edelman found when he used the packet sniffer to locate a private, unpublished URL, Mr. Edelman would not have been able to “reverse engineer” the SaveNow Code. The elaborate efforts by a paid consultant on behalf of a private litigant to penetrate the protections carefully created by WhenU should not deprive WhenU of the protection to which its proprietary software is entitled.

B. The Testimony of Mr. Naider Which Reveals the Actual Workings of the SaveNow Code Should Be Sealed

As described above, WhenU considers the SaveNow Code a confidential and proprietary trade secret and treats it as such. The SaveNow Code is not known to the general public or to WhenU’s competitors, and revelation of the Code and its actual workings would cause WhenU a substantial competitive injury. Tr. VII (Naider) 71:24-72:12.

Although WhenU would not ordinarily reveal anything about the operation of the SaveNow Code, its CEO Avi Naider testified about the SaveNow Code at length in order to correct the many misstatements about the Code made by Mr. Edelman during his testimony. Mr. Naider provided a thorough explanation of the SaveNow category system for mapping ads; he also testified about various entries in the Directory and their functionality. None of this is public information, and none of this was revealed to advance any claim being asserted by WhenU, the defendant in this case. Even Mr. Edelman conceded, following Mr. Naider’s testimony, that he had erred in his earlier testimony and had learned things that – with all the time, resources, packet sniffers and expertise he brought to bear – he had not been able to deduce for himself.

Accordingly, there can be no question that Mr. Naider’s testimony divulged information “not [] readily ascertainable by proper means” that is “the subject of efforts that are

reasonable under the circumstances to maintain its secrecy," Mich Stat. Ann. § 445.1902, and is therefore a trade secret. Since the information was only divulged by Mr. Naider as necessary to defend this action, the Court should continue the Order sealing certain portions of Mr. Naider's testimony.

CONCLUSION

For the reasons set forth above, defendant respectfully submits that the Court should continue the Order sealing the Edelman Declaration and the confidential portions of testimony of Mr. Naider and Mr. Edelman.

Respectfully submitted,

BUTZEL LONG

By: 

Leonard M. Nichoff (P36695)

Attorneys for Defendant
350 South Main Street, Suite 300
Ann Arbor Michigan 48104
(734) 995-3110

KRONISH LIEB WEINER & HELLMAN LLP

Attorneys for Defendant
Celia Goldwag Barenholtz
Michael Paley
Jason Koral
1114 Avenue of the Americas
New York, New York 10036
(212) 479-6000

Dated: October 9, 2003